Università degli Studi di Parma
Dipartimento di Ingegneria e Architettura

Family name (cognome)	Name (nome)	Student ID number (matricola)
[redacted]	[redacted]	[redacted]

Cybersecurity
Exam 22/6/2023

1) **What is a *known-plaintext* attack?**
- An attack scheme to a cryptographic system where the attacker can choose some messages m_i and, for each m_i, he can capture the corresponding ciphertext $c_i = E_K(m_i)$
- An attack scheme to a cryptographic system where the attacker can choose some ciphertext messages c_i and, for each c_i, she can obtain the corresponding cleartext $m_i = D_K(c_i)$
- An attack scheme to a cryptographic system where the attacker can capture some ciphertexts messages $c_i = E_K(m_i)$ and, for each c_i, he can obtain the corresponding cleartext m_i

DSA is:
- A symmetric block cipher algorithm
- An asymmetric block cipher algorithm
- A hash algorithm
- A signature algorithm

2) **Given a block cipher E in CBC mode, with block size *r* and key length *n*, let (m_i, c_i) a pair of plaintext and ciphertext, with message length *tr*. Which is the complexity of a brute force attack against the secret key, in terms of number of single block encryption operations, supposing that in each attempt the entire message is processed:**
- n 2^r
- tr*n*
- tr 2^n
- t 2^n

3) **What do you need in order to verify the validity of a digital certificate?**
- the certificate of the CA that signed the given certificate
- the private key of the CA that signed the given certificate
- your own certificate

4) **Which is the advantage to use sequence numbers, timestamps, or random values, in an authentication scheme?**
- to protect against brute force attack
- to protect against replay or reflection attacks
- to increase the security, in case of password too short
- to distinguish request messages from responses

5) **Which service is NOT provided by IPSec ESP?**
- confidentiality
- delivery confirmation
- data integrity check
- protection against replay attacks

6) **What is a Spoofing attack?**
- listening on the transmission medium along the path between two entities that are communicating
- forcing a system (the victim) to send the data unencrypted rather than encrypted
- sending data with a false sender address, impersonating the identity of another system

7) **Let us consider the following cleartext:**

m = 1100 0000 1100 0000

It is sent encrypted with a symmetric block encryption algorithm $E_K(\cdot)$, with block size equal to 4bit, with key K, using OFB concatenation mode with IV=0001. The complete substitution table of $E_K(\cdot)$ with key K is reported her on the right. The resulting cipher text is:

c = 1000 0010 0001 1001 (IV=0001)

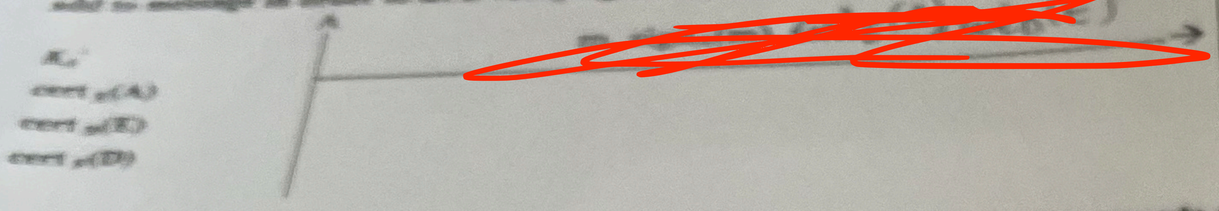
plaintext	ciphertext
0000	1110
0001	0100
0010	1101
0011	000
0100	00
0101	1
0110	
0111	
1000	
1001	
1010	
1011	
1100	
1101	
1110	
1111	

Please indicate the value of the modified ciphertext c' and IV' such as the corresponding cleartext (when decrypted with the same key K) will be:

m'= 1100 0000 1001 0000

Response: c = [redacted] (IV' = [redacted])

13) An entity A wants to send a message m to B signed with her private key K_A^-. Consider that A has her own private key K_A^-, the $cert_A(A)$, $cert_A(E)$, and the $cert_A(D)$, while B has $cert_C(E)$, $cert_C(D)$, $cert_C(C)$. Which information should A add to message in order to let B verifying the signature?



K_B^+
$cert_C(B)$
$cert_C(D)$
$cert_C(C)$

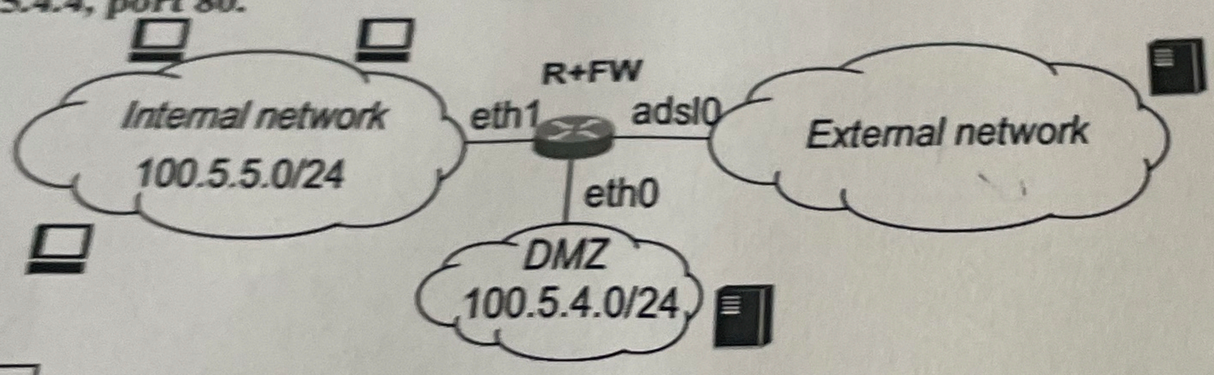
14) The entity A wants to anonymize a message m to be sent to D, by using the cascade of high-latency anonymizing Mix nodes B and C, in such a way that A→B→C→D is the sequence of nodes that will be involved in the delivery. Assume that K_i^+ and K_i^- are the public and private keys of node *i* (with *i*=A,B,C,D). What is a possible message that A will send to B for such a purpose?

15) Let us consider the following network topology. You are requested to configure the packet filtering router (FW) so that:

a) it is possible to communicate in HTTP from any client of the internal network to any server of the external network, limited to server port 80;

b) it is allowed any communication between any node of the internal network and DMZ;

c) it is possible to establish client/server communications from any node (client) of the external network to the HTTP server 100.5.4.4, port 80.

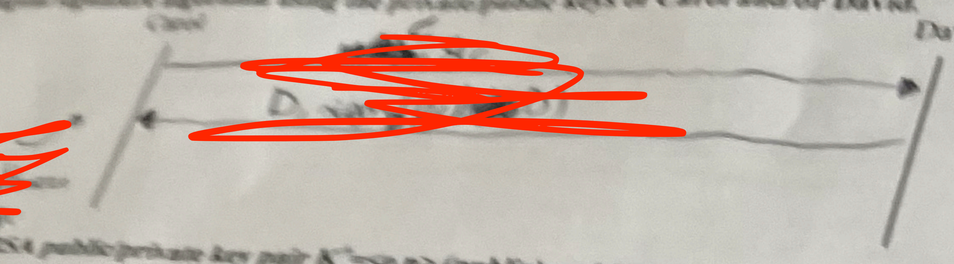


FORWARD

matching						action
src_addr	dest_addr	proto	src_port	dest_port	conn_state (NEW / ESTABLISHED)	ACCEPT/ DROP

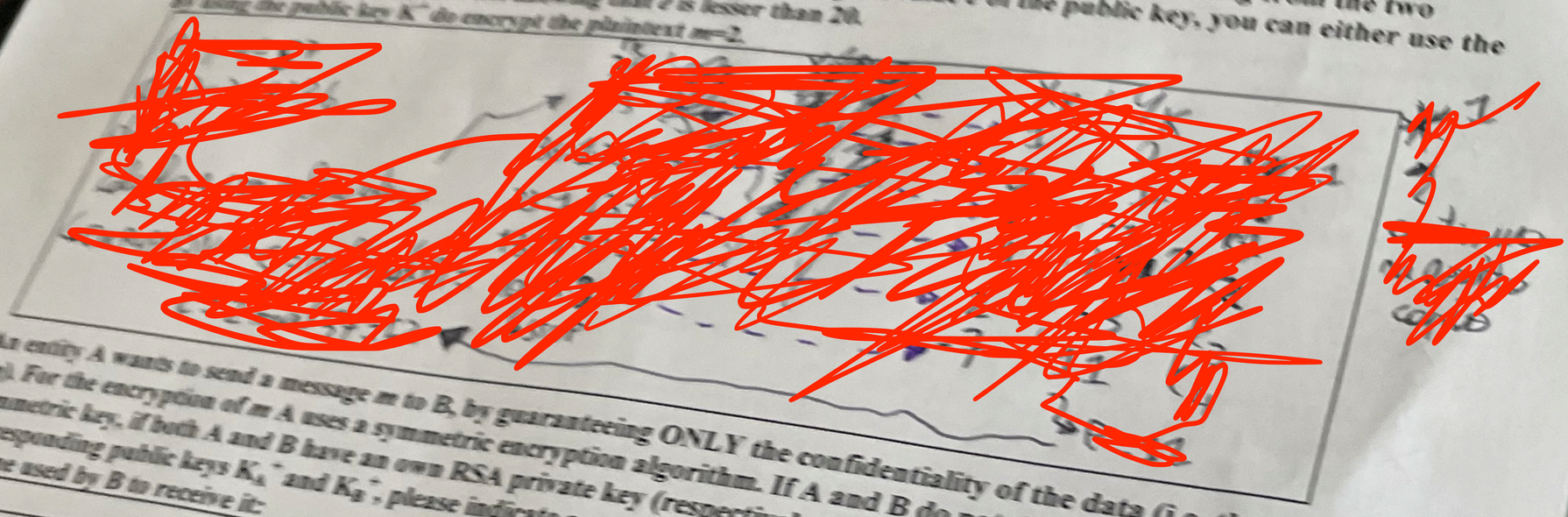
9) What is static VAR control?

10) Show a possible challenge-response authentication scheme that can be used by Carol to authenticate David, based on a digital signature algorithm using the private/public keys of Carol and/or David.



10) Create a pair of RSA public/private key pair $K^+=<e,n>$ (public) and $K^-=<d,n>$ (private), starting from the two secret prime numbers $p=3$, $q=19$, and value $d=23$. For obtaining the value e of the public key, you can either use the Euclid's algorithm or try and test knowing that e is lesser than 20.

b) using the public key K^+ do encrypt the plaintext $m=2$.



11) An entity A wants to send a message m to B, by guaranteeing ONLY the confidentiality of the data (i.e. the message m). For the encryption of m A uses a symmetric encryption algorithm. If A and B do not share in advance any symmetric key, if both A and B have an own RSA private key (respectively K_A^- and K_B^-), and if they share the corresponding public keys K_A^+ and K_B^+, please indicate a possible scheme used by A to send the message and the scheme used by B to receive it:

Sender side	Receiver side
Data actually sent:	

12) Show the Diffie-Hellman exchange between Carol and David, using the generator $g=2$, the prime $p=13$, and the values $x_C=4$ and $x_D=5$ as secret values of Carol and David, respectively. Indicate the exchanges values y_C and y_D, and the resulting DH secret computed separately by Carol and David.